25X1 [redacted]

Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8

CONFIDENTIAL

OC-0913 4/76

15 July 1976

MEMORANDUM FOR: OC Equipment Board Members

25X1 FROM : [redacted]
Secretary, OC Equipment Board

SUBJECT : Minutes of OC Equipment Board Meeting No. 2-76

1. Meeting No. 2-76 of the OC Equipment Board was held on 13 July 1976. The following persons were in attendance:

[redacted] 25X1

25X1 2. [redacted] introduced the agenda items and advised that the briefing was primarily for information purposes. Mr. 25X1 [redacted] then proceeded to describe the Data Encryption Standard (DES), an algorithm developed under the auspices of the National Bureau of Standards (NBS) to satisfy the requirements for protection of an individual's privacy in Federal computer systems and networks as specified in the Privacy Act. The DES program was initiated by NBS in 1972 and early development was accomplished in-house. A 1973 NBS decision to utilize external contractors in this endeavor resulted in the awarding of a contract to IBM. The initial DES design by IBM was reviewed during 1975 and a final revised standard was accepted in December 1975. The entire program has been publicized and will be commercially available

[redacted] 25X1

[redacted] 25X1

Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8

CONFIDENTIAL

Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8

SUBJECT: Minutes of OC Equipment Board Meeting No. 2-76 25X1

[redacted]

While the system appears technically sound, the entire program is enmeshed in politics. The Department of Commerce, parent organization of NBS, has requested a cost analysis to determine the impact on computer equipment manufacturers before approving the logic as a Federal standard. Representatives of Stanford Research Institute have stated that the system is weak and claim to have developed a box to break the code. NSA reviewed the claims and stated that the procedures used are impractical and the DES is still considered a high grade system. NSA has stated that the DES is not intended for voice privacy applications, however, the method of controlling this was not immediately apparent. NSA has not exercised export control on this device, claiming that to do so would just further other development in this area. Although NSA has been relatively free with information regarding DES, it is felt that the full story pertaining to the security of the logic has not been attained. NSA is supposed to issue a policy paper on the system in the next 60-90 days. A number of congressional groups are also looking into the DES to ensure that the protection afforded the individual is adequate. They have also inquired about the relationship of NSA to the development of the system.

25X1 [redacted] concluded that, in view of the political ramifications, we should take a very passive role in this development and not pursue the investigation for Agency voice privacy use at this time.

3. The second and last agenda item concerning the KG-84 cryptographic system was introduced by [redacted] who stated that 25X1
the problems to be discussed were uncovered as a result of OC-CS attempts to get an early in-depth look at the auto-key features of
25X1 this system. [redacted] then proceeded to describe the general features of the KG-84. The KG-84 is a dedicated loop encryption device that is part of the overall Tenley program and features remote rekeying and variable update. It uses the Saville family of cryptologic, the same used in the Vinson program. There are three crypto variables - an update variable (daily), a new traffic variable (monthly), and a rekeying variable (3 months - 1 year). The rekeying and daily variables are updated manually on-site, whereas the monthly variable is usually updated electrically from the remote end. The KG-84 can be used in two network

Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8

25X1 [redacted]

CONFIDENTIAL

Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8

SC-0913 4/76

SUBJECT: Minutes of OC Equipment Board Meeting No. 2-76

[redacted] 25X1

4. With no other business to discuss, the meeting was adjourned.

[redacted] 25X1

Distribution:
1 - DD/CO
1 - C/OC-O
1 - C/OC-E
1 - C/OC-S
1 - C/OC-CS
1 - C/OC-P&B
1 - Board Secretary

25X1 MINUTES APPROVED:

[redacted]

Deputy Director of Communications

7.16.74
Date

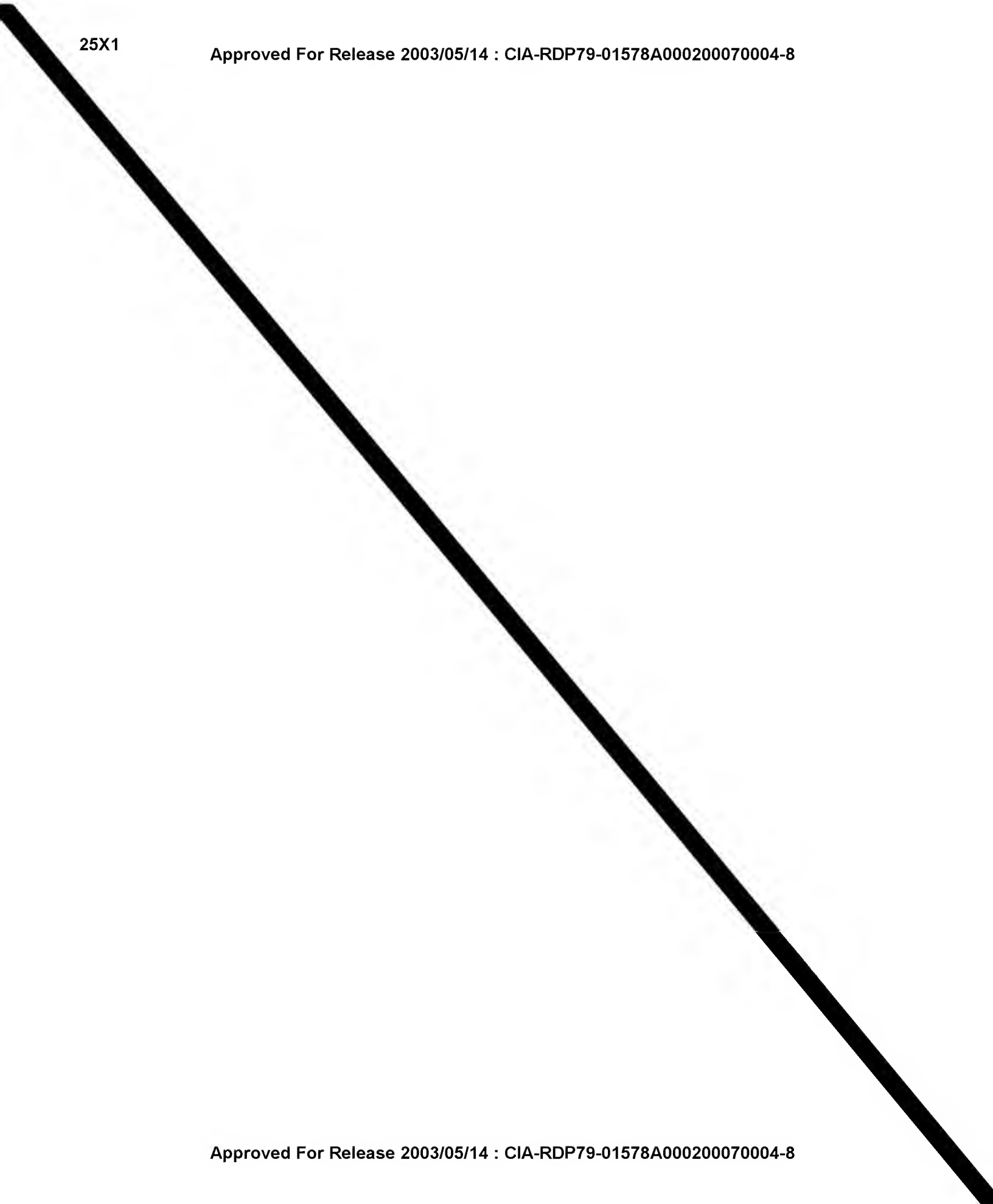
25X1 [redacted]

CONFIDENTIAL

Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8

25X1

Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8



Approved For Release 2003/05/14 : CIA-RDP79-01578A000200070004-8